OZ

# Security system for data transmission in electronic payment transactions

**Publication number:** DE19634418
**Publication date:** 1998-03-05
**Inventor:** LEWKE KLAUS-DIETER DR (DE)
**Applicant:** ORGA CONSULT GMBH (DE)
**Classification:**
**- international:** ***G07F7/10;*** **G07F7/10**; (IPC1-7): G06F17/60; G06K19/07; G07F7/08; G07F19/00
**- european:** G07F7/10D4T
**Application number:** DE19961034418 19960826
**Priority number(s):** DE19961034418 19960826



Abstract of **DE19634418**

The use of a card in a terminal results in an electronic receipt being generated based on the data stored in the chip of the card. The data is used in a security module built into the terminal and this controls the transaction

FG

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 196 34 418 A1**

(51) Int. Cl.[6]:
**G 06 F 17/60**
G 06 K 19/07
G 07 F 7/08
G 07 F 19/00

(21) Aktenzeichen: 196 34 418.2
(22) Anmeldetag: 26. 8. 96
(43) Offenlegungstag: 5. 3. 98

(71) Anmelder:
Orga Consult GmbH, 33104 Paderborn, DE

(72) Erfinder:
Lewke, Klaus-Dieter, Dr., 33100 Paderborn, DE

(56) Entgegenhaltungen:
US 55 21 363

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zur Sicherung der Datenübertragung im elektronischen Zahlungsverkehr

(57) Die Erfindung bezieht sich auf Verfahren zur Sicherung der Datenübertragung im elektronischen Zahlungsverkehr mittels eines mobilen Datenträgers, insbesondere einer Chipkarte, an Dienstanbieterendgeräten, die nicht dauerhaft mit einem Abrechnungs-/Kontoführungssystem verbunden sind, wobei die Anwendung der mobilen Datenträger elektronische Belege erzeugt, dadurch gekennzeichnet, daß
- ein Exemplar des elektronischen Beleges auf dem mobilen Datenträger gespeichert wird,
- und dieser Beleg bei mindestens einer weiteren Anwendung des mobilen Datenträgers an ein weiteres Endgerät zur Weiterleitung an das Abrechnungs-/Kontoführungssystem übergeben wird.

DE 196 34 418 A1

DE 196 34 418 A1

Beschreibung

Die Erfindung bezieht sich auf Verfahren zur Datenübertragung im elektronischen Zahlungsverkehr.

Im elektronischen Zahlungsverkehr weist sich ein Käufer durch einen mobilen Datenträger aus, z. B. eine Chipkarte. Das Unternehmen, welches die bargeldlose Dienstleistung anbietet und ggf. die Datenträger zur Verfügung stellt, wird im folgenden als Herausgeber bezeichnet. Das Rechensystem des Herausgebers veranlaßt die Banktransaktionen, welche mit dem bargeldlosen Bezahlen verbunden sind. Diese Rechensystem wird im folgenden als Abrechnungssystem oder Kontoführungssystem bezeichnet.

In der Regel ist ein Kassenterminal (Dienstanbieterendgerät) an das Abrechnungssystem angeschlossen, z. B. über eine Telefonleitung. Wird ein Vorgang über eine geschaltete Leitung abgewickelt, spricht man von Online-Verarbeitung, sonst von Offline-Verarbeitung.

Über eine Online-Verbindung zum Abrechnungssystem können gestohlene oder verlorengegangene Datenträger von der Weiterverwendung ausgeschlossen werden, indem gegen eine Sperrliste geprüft wird. Auch für die Abwicklung der Buchungen ist die sofortige Übertragung der Buchungssätze an das Abrechnungssystem am sichersten. Datensätze können so nicht verloren gehen.

Wegen der Leitungskosten ist Online-Prüfung jedes einzelnen Datenträgers jedoch nicht wirtschaftlich. Daher werden Datenträger nur sporadisch online geprüft und Buchungssätze gesammelt. Diese elektronischen Belege werden dann in Paketen übertragen, vorzugsweise zu Zeiten niedriger Leitungskosten.

Deshalb beinhaltet jedes Kassenterminal ein Sicherheitsmodul, welches der Herausgeber zur Verfügung stellt. Dieses Sicherheitsmodul prüft die Echtheit der Datenträger und speichert die Buchungssätze in sicherer Weise. Es sind verschiedene Sicherheitsverfahren bekannt. Zum Teil beruhen die Verfahren auf Kryptographie, wobei die benötigten Schlüssel in den Sicherheitsmodulen und mobilen Datenträgern (z. B. Chipkarten) gegen Auslesen geschützt sind. Die Sicherheitsmodule (evtl. auch die Datenträger selbst) erzeugen elektronische Unterschriften für die Datensätze, welche zur Abwicklung der Banktransaktionen übermittelt werden. Dadurch wird verhindert, daß Nachrichten unbemerkt manipuliert werden können.

Entsprechende Verfahren sind aus dem ec-Cash-System und anderen Systemen bekannt.

Einige Terminals besitzen u. U. gar keine Möglichkeit, jederzeit Online-Verbindungen herzustellen. Dies gilt insbesondere für mobile Terminals in Verkaufsfahrzeugen. Eine naheliegende Lösung ist, auch hier die Buchungen im Sicherheitsmodul zu sammeln. Um die elektronischen Belege an das Abrechnungssystem zu übertragen, wird der Sicherheitsmodul von Zeit zu Zeit an ein Übertragungsgerät angeschlossen. Die Akzeptanzstelle (Dienstanbieter) ist gezwungen dies zu tun, um das Geld für die verkauften Waren zu erhalten.

Selbst wenn ein möglicher Angreifer die mobilen Datenträger und Sicherheitsmodule technisch nicht verändern kann, ist betrügerischer Mißbrauch unter Umständen trotzdem möglich. Nämlich dann, wenn verhindert wird, daß gespeicherte Nachrichten aus dem Sicherheitsmodul zum Abrechnungssystem übertragen werden.

Für Bezahlsysteme auf Basis von Chipkarten werden unter anderem die folgenden beiden Bezahlarten diskutiert:

- Kreditorische Börse: Der Betrag wird vom Konto des Käufers abgebucht. Um Bezahlung zu sichern, kann ein Kreditrahmen im Datenträger gespeichert sein, welcher um den Kaufbetrag vermindert wird.
- Vorausbezahlte Börse (Prepaid-Börse): Ein Geldbetrag wird im voraus an den Herausgeber gezahlt und auf der Karte gespeichert.

Beide Verfahren zeigen in gewissen Situationen Vorteile auf. Der Inhaber des Datenträgers will meist sehr große Geldbeträge nicht im voraus bezahlen. Größere Geschäfte wickelt er deshalb mittels einer kreditorischen Börse ab. Für die Erfindung ist nicht von Belang, ob der Wert der elektronischen Börse einem eingezahlten Betrag oder einem Kreditrahmen (Überziehungskredit) entspricht. Bezahlung aus der kreditorischen Börse entspricht der Ausstellung eines Schecks, den die Akzeptanzstelle einlöst. Durch die Aktualisierung des gespeicherten Betrags wird verhindert, daß der Inhaber sein Konto oder einen vorgegebenen Kreditrahmen überzieht.

Da Transaktionen über (Bank-)Konten mitgeführt werden, verliert der Inhaber Geld aus kreditorischen Börsen nicht bei Verlust oder Defekt des mobilen Datenträgers.

Die Kosten für die Banktransaktion, welche mit dem Bezahlen aus der kreditorischen Börse verbunden sind, lassen sich für kleine Geldbeträge jedoch nicht rechtfertigen. Hier bietet es sich an, Beträge aus Kleingeldbörsen in den Sicherheitsmodul der Kassenterminals einfach aufzusummieren und von Zeit zu Zeit den Gesamtbetrag zu übermitteln. Bei Verlust oder Defekt kann der Inhalt der Kleingeldbörse nicht ersetzt werden, da ja gerade die Verwaltung der notwendigen Information eingespart wird. Bezahlung aus der Kleingeldbörse kann daher am ehesten mit dem Bezahlen durch Bargeld verglichen werden. Die Herkunft des Geldes ist nicht mehr feststellbar und mit dem Verlust des mobilen Datenträgers ist auch das Geld verloren, genauso wie bei dem Verlust eines Portemonnaies.

Umbuchungen von der kreditorischen Börse in die Kleingeldbörse am Händlerterminal sind aus verschiedenen Gründen wünschenswert. Die entsprechende Umbuchung kann mit Hilfe des Sicherheitsmodul vor Manipulationen geschützt werden. Der elektronische Umbuchungsbeleg wird einfach mit den Abrechnungen der Akzeptanzstelle durch das Sicherheitsmodul eingereicht.

Verfahren zur Umbuchung zwischen verschiedenen Börsen in Chipkarten sind aus DE 42 43 851 bekannt.

Im Vergleich mit Bankgeschäften, die durch Papierbelege ausgeführt werden, entspricht diese Umbuchung einer Barabhebung. Hier wird deutlich, daß der Beleg für den Herausgeber sehr wichtig ist. Denn trifft der Beleg nicht beim Herausgeber ein, verliert der Herausgeber das umgebuchte Geld.

Wird die Umbuchung online durchgeführt, besteht keine Gefahr von Mißbrauch. Wird die Buchung aber offline durchgeführt, kann der Betreiber des Terminals den Eingang des Belegs im Abrechnungssystem verhindern. Er schließt einfach das Terminal nicht an die Übertragungsleitung an.

Ein Angreifer (Betrüger) kann auf folgende Weise vorgehen. Er verschafft sich ein Terminal mit Sicherheitsmodul für Offline-Betrieb und einen oder mehrere

mobile Datenträger. Der Angreifer kann an diese Geräte durch Diebstahl oder als Teilnehmer an den betreffenden Diensten gelangen. Der Angreifer veranlaßt mittels seines Sicherheitsmoduls die Umbuchung in die Kleingeldbörse. Er verhindert, daß der elektronische Beleg an das Abrechnungssystem weitergeleitet wird. Da der Ursprung von Beträgen aus Kleingeldbörsen nicht kontrolliert wird, kann der Angreifer die Kleingeldbörse leerräumen. Der Datenträger wird als verloren gemeldet, so daß der Herausgeber dem Angreifer den Betrag erstattet, welcher ursprünglich gespeichert war.

Aufgabe der Erfindung ist es, den Eingang von elektronischen Belegen sicherzustellen (bzw. die Verlustwahrscheinlichkeit des Belegs zu minimieren) und so Betrug zu verhindern.

Generell sind diese Prinzipien geeignet, für beliebige Typen von Belegen größere Sicherheit gegen Verlust zu schaffen. Dabei ist unerheblich, ob der Verlust durch Defekt, Diebstahl oder durch Betrug entsteht. Ebenso unerheblich ist, ob ein Betrugsversuch auf anderen Prinzipien als den beschriebenen beruht.

Die Erfindung reduziert die Möglichkeiten des Verlustes von Belegen und Betrug durch herbeigeführten Verlust mittels folgender Gegenmaßnahmen:

a) Beschränkung der Umbuchungen: Die Anzahl und/oder Höhe der Buchungen von der kreditorischen Börse in die Kleingeldbörse wird beschränkt. Dadurch wird der Schaden limitiert. Die Beschränkung und die Anzahl bzw. Höhe der Buchungen, welche bereits vorgenommen wurden, wird im Datenträger gespeichert.

b) Speicherung von Buchungen im Datenträger: Elektronische Belege über Umbuchungen und andere Transaktionen aus der kreditorischen Börse werden zusätzlich im Datenträger selbst abgelegt. Damit erreichen die Belege das Abrechnungssystem, wenn der Inhaber die Karte nachlädt.

e) Übertragung der Belege durch Online-Terminals: Gelangt der Datenträger während eines Bezahlvorgangs an ein Online-Terminal, wird der Beleg direkt übertragen. (Dies setzt Speicherung nach b) voraus.) Nach der Übertragung wird der Beleg aus dem Datenträger entfernt, bzw. als übertragen gekennzeichnet.

d) Übertragung durch Offline-Terminals: Bei der Benutzung des Datenträgers an einem weiteren Offline-Terminals wird der Beleg über die Umbuchung ins Sicherheitsmodul übertragen. Der Beleg gelangt zum Abrechnungssystem bei der normalen Übertragung der Einnahmen. Dieser Übertragungsweg wird an mehreren Offline-Terminals versucht. Spätestens nach einer Online-Übertragung werden keine weiteren Versuche mehr unternommen. Voraussetzung für das Verfahren ist eine eindeutige Kennung des Belegs, so daß mehrfaches Eintreffen toleriert werden kann.

Um Leitungskosten und Verarbeitungskosten durch mehrfaches Übermitteln des Belegs einzuschränken, muß die Zahl der Speicherungen in Terminals beschränkt werden. Ob der Beleg tatsächlich in ein bestimmtes Terminal übertragen wird, wird deshalb mit Hilfe einer Regel bestimmt. Diese Regel kann einen Zufallszahlengenerator enthalten. Der Angreifer ist dann nie sicher, daß er die Übertragung (in seinem eigenen Terminal) abfangen kann.

Der Herausgeber kann die Weiterleitung von Belegen vergüten und so für die Akzeptanzstellen attraktiv machen. Wirksamer sind jedoch Methoden, welche die Erlangung des legalen wirtschaftlichen Nutzens an die Übertragung von Belegen gekoppelt wird, deren Unterdrückung zu Betrug genutzt werden kann. D.h. Akzeptanzstellen werden die Übertragung aller Belege aus dem Sicherheitsmodul dann vornehmen, wenn ihr wirtschaftlicher Nutzen durch legale Geschäfte den möglichen betrügerischen Gewinn übersteigt. Man kann auch davon ausgehen, daß das Verhalten solider Akzeptanzstellen sich in der Zukunft fortsetzt. Darauf beruhen weitere Verfahren.

e) Reihenfolge der Übertragung aus den Sicherheitsmodulen: Das Sicherheitsmodul überträgt zuerst Daten über Umbuchungen. Versucht eine betrügerische Akzeptanzstelle die Übertragung der Umbuchungsbelege zu verhindern, muß sie auf Einnahmen durch Übertragung ihrer Verkaufsbelege verzichten.

f) Bevorzugung von Terminals, in welchen hohe Beträge gespeichert sind: Eine Akzeptanzstelle hat ein besonders großes Interesse Buchungen aus den Sicherheitsmodulen zu übertragen, wenn bereits hohe Beträge aufgelaufen sind. Eine Übertragung in diese Sicherheitsmodule führt mit größerer Sicherheit zu einer Übertragung an das Abrechnungssystem.

g) Bevorzugung von Terminals mit bisher häufiger Übertragung: Es kann hier angenommen werden, daß mit großer Wahrscheinlichkeit der Beleg weitergeleitet wird.

h) Blockierung der Umbuchung durch das Sicherheitsmodul: Das Terminal bzw. das Sicherheitsmodul blockiert weitere Umbuchung, wenn Mißbrauch vermutet werden kann. Dies kann angenommen werden, wenn

— eine vorgebene Anzahl von Umbuchungen, bzw. eine Summe überschritten wird,

— Summen, die durch Umbuchungen bewegt werden einen gewissen Anteil an anderen Umsätzen übersteigen.

Durch Übertragung der Belege kann das Terminal wieder entblockiert werden. Die Blockierung kann auf die Funktionen beschränkt werden, welche zu Betrug genutzt werden können. Die Blockierung kann auch dann zurückgenommen werden, wenn während der Weiterbenutzung entsprechende Belege gespeichert wurden, welche die Betrugsvermutung entkräften.

Dieses Verfahren limitiert zumindest die Höhe des Betrugs.

i) Aufhebung von Blockierungen: Die Blockierung eines Datenträgers kann zurückgenommen werden, wenn sie durch Belege begründet war, die inzwischen an das Abrechnungssystem übertragen wurden.

Natürlich müssen auch bei der Übertragung von Umbuchungsbelegen Leitungskosten berücksichtigt werden. Übertragungen des Umbuchungsbelegs in Sicherheitsmodule von Offline-Terminals, wie in b) beschrieben, ist daher nicht bei jeder Buchung wünschenswert. Wenn der Beleg das Abrechnungssystem bereits erreicht hat, sollte weiteres Versenden eingestellt werden. Eine Methode beschreibt Verfahren j).

j) Wiedererkennung von Datenträger und Sicherheitsmodul: Im Datenträger wird vermerkt, an welche Sicherheitsmodule Belege übertragen wurden. Der Karteninhaber sucht in der Regel gewisse Akzeptanzstellen häufig auf (z. B. den Laden an der Ecke). Wenn der Beleg nicht mehr im Sicherheitsmodul abgelegt ist, wurde der Beleg an das Abrechnungssystem abgeschickt. Im Datenträger kann der entsprechende Beleg dann gelöscht, bzw. als übertragen markiert werden.

k) Wiedererkennung sicherer Überträger: Falls Verfahren i) angewendet wird, kann leicht vermutet werden, daß das betreffende Terminal zuverlässig Belege weiterleitet und unnötige Verbreitung des Beleges durch Verfahren i) mit hoher Wahrscheinlichkeit beschränkt wird. Der Datenträger selbst kann eine Liste dieser Terminals verwalten und diese Information zukünftig berücksichtigen.

Die vorstehenden Verfahren sind so beschrieben, daß in den Datenträgern nur Belege gespeichert sind, welche bei Anwendung dieses Datenträgers erzeugt wurden. Dies ist jedoch keineswegs notwendig. Bei Anwendung eines Datenträgers kann das Terminal Belege, die durch Anwendung anderer Datenträger entstanden sind, in Datenträger speichern und so die Weiterleitung veranlassen. Der Datenträger verteilt diesen Beleg dann nach den gleichen Prinzipien weiter, wie er dies für seine eigenen Belege tut. Übertragungsversuche können und sollten in sinnvoller Weise durch die Verfahren beschränkt werden, die oben erläutert wurden.

Besonders wichtig für die praktische Anwendung der Verfahren ist Ausgewogenheit zwischen Sicherheit und Kosten, in diesem Zusammenhang die Übertragungskosten. Zu häufige Übertragungen treiben die Kosten in die Höhe und können sogar den Vorteil von Kleingeldbörsen, nämlich die Einsparung von Leitungskosten, aufheben. Zu wenige Übertragungen, im Extremfall gar keine, erlauben Betrug. Falls die Regel zu starr festgelegt wird, kann ein Angreifer die Übertragung abfangen, indem er die betreffenden Anwendungen auf seinem Terminal ausführt und dieses Gerät nicht zur Übertragung an das Abrechnungssystem anschließt.

Wird die Speicherung in ein Terminal von Bedingungen abhängig gemacht, die der Angreifer nicht vorhersehen kann, kann er das Eintreffen des Belegs im Abrechnungssystem nicht sicher verhindern. Um Unvorhersagbarkeit zu realisieren, kann ein Zufallszahlengenerator verwendet werden. Zufallszahlengeneratoren sind aus der Literatur bekannt.

Eine einfache Regel, die festlegt, ob ein Beleg übertragen wird, kann so festgelegt werden:

1) Verschiedene Bewertungskriterien können zur Berechnung einer Schranke s herangezogen werden, z. B. so daß
- s mit der Anzahl bisheriger Speicherungen steigt,
- s mit der Anzahl bisheriger Speicherungen in "sichere Terminals" steigt
- s mit der Anschlußhäufigkeit des Terminals sinkt,
- s mit dem Buchgeldbetrag sinkt, welcher im Terminal gespeichert ist,
- s mit der Übertragungssicherheit durch das Terminal sinkt,
- s mit der Höhe der vorzunehmenden Abbuchung aus der Kleingeldbörse sinkt.

2) Mit dem Zufallszahlengenerator wird eine Zahl r berechnet. Nur falls r > s, wird die Übertragung vorgenommen.

Regeln nach diesen Kriterien bevorzugen Terminals, die mit großer Wahrscheinlichkeit Weiterleitung an das Abrechnungssystem veranlassen. Andererseits sinkt die Wahrscheinlichkeit einer Speicherung mit der Zeit, so daß die Anzahl der Übertragungen schon durch die Regel limitiert wird. Der Teil der Bewertung, der durch bisherige Übertragungen bestimmt ist, kann im Datenträger selbst abgelegt werden. Die Bewertung sei im Datenfeld w abgelegt. Der Herausgeber setzt w auf einen Initialwert. w wird nach jeder Speicherung inkrementiert, abhängig von einer Bewertung der erfolgten Übertragung. D.h. falls das Terminal als sicherer Überträger eingestuft wird, fällt die Erhöhung stärker aus.

## Patentansprüche

1. Verfahren zur Sicherung der Datenübertragung im elektronischen Zahlungsverkehr mittels eines mobilen Datenträgers, insbesondere einer Chipkarte, an Dienstanbieterendgeräten, die nicht dauerhaft mit einem Abrechnungs-/Kontoführungssystem verbunden sind, wobei die Anwendung der mobilen Datenträger elektronische Belege erzeugt, dadurch gekennzeichnet, daß
   - ein Exemplar des elektronischen Beleges auf dem mobilen Datenträger gespeichert wird,
   - und dieser Beleg bei mindestens einer weiteren Anwendung des mobilen Datenträgers an ein weiteres Endgerät zur Weiterleitung an das Abrechnungs-/Kontoführungssystem übergeben wird.

2. Verfahren nach Patentanspruch 1 dadurch gekennzeichnet, daß der elektronische Beleg jeweils an ein Endgerät übergeben wird, das mit dem Abrechnungs-/Kontoführungssystem verbunden ist oder mit diesem eine Verbindung unmittelbar herstellen kann, und der Beleg unverzüglich an das Abrechnungs-/Kontoführungssystem weitergeleitet wird.

3. Verfahren nach Patentanspruch 1 dadurch gekennzeichnet, daß der elektronische Beleg jeweils an ein Endgerät übergeben wird, das nicht dauerhaft mit dem Abrechnungs-/Kontoführungssystem verbunden ist, und bei wiederholter Anwendung des mobilen Datenträgers in demselben Endgerät festgestellt wird, ob der Beleg an das Abrechnungs-/Kontoführungssystem übertragen wurde, und bei erfolgter Übertragung an das Abrechnungs-/Kontoführungssystem weitere Übertragungen vom mobilen Datenträger in Endgeräte unterbleiben.

4. Verfahren nach einem der vorstehenden Patentansprüche dadurch gekennzeichnet, daß zur Reduzierung von Übertragungskosten durch eine vorbestimmte Regel oder durch eine Regel, welche einen Zufallszahlengenerator oder eine andere Methode zur Generierung zufälliger Werte verwendet, bestimmt wird, ob der elektronische Beleg zur Weiterleitung an das Abrechnungs-/Kontoführungssystem in das Endgerät übertragen wird, mit dem der Datenträger aktuell angewendet wird.

5. Verfahren nach Patentanspruch 4 dadurch gekennzeichnet, daß der elektronische Beleg durch die Regel bevorzugt an solche Endgeräte übertra-

gen wird, für die hohe Wahrscheinlichkeit für die Übertragung an das Abrechnungs-/Kontoführungssystem abgeleitet werden kann.

6. Verfahren nach Patentanspruch 5 dadurch gekennzeichnet, daß der elektronische Beleg durch die Regel bevorzugt an solche Endgeräte übertragen wird, in denen bereits Belege gespeichert sind, deren Übertragung an das Abrechnungs-/Kontoführungssystem für den Betreiber des Endgeräts einen hohen wirtschaftlichen Nutzen erbringt.

7. Verfahren nach Patentanspruch 5 dadurch gekennzeichnet, daß der elektronische Beleg durch die Regel bevorzugt an Endgeräte mit hoher Anschlußhäufigkeit an das Abrechnungs-/Kontoführungssystem übertragen wird.

8. Verfahren nach Patentanspruch 5 dadurch gekennzeichnet, daß

— im mobilen Datenträger Informationen über erfolgte Weiterleitungen elektronischer Belege durch Endgeräte an das Abrechnungs-/Kontoführungssystem gespeichert werden und

— durch die Regel solche Endgeräte bevorzugt werden, die bisher erkennbar Belege an das Abrechnungs-/Kontoführungssystem weitergeleitet haben.

9. Verfahren nach Patentanspruch 4 dadurch gekennzeichnet, daß durch die Regel die Anzahl vorgenommener Speicherungen in Endgeräte berücksichtigt werden, so daß die Wahrscheinlichkeit der Speicherung in weitere Endgeräte mit der Zeit sinkt.

10. Verfahren gemäß Oberbegriff von Anspruch 1 dadurch gekennzeichnet, daß bei einem Endgerät, welches nicht dauerhaft an das Abrechnungs-/Kontoführungssystem angeschlossen ist, bei einer Übertragung von elektronischen Belegen vor der Übertragung von Belegen, welche für den Betreiber des Endgerätes einen wirtschaftlichen Nutzen erbringen, solche elektronischen Belege an das Abrechnungs-/Kontoführungssystem übertragen werden, deren Nichtweiterleitung einen Betrug ermöglicht oder-die aus anderen Gründen zur Weiterleitung an das Abrechnungs-/Kontoführungssystem in das Endgerät eingespeichert wurden.

11. Verfahren gemäß Oberbegriff von Anspruch 1 dadurch gekennzeichnet, daß ein Endgerät elektronische Belege unverzüglich an das Abrechnungs-/Kontoführungssystem überträgt oder eine weitere Anwendung mit mobilen Datenträgern sperrt, bis eine Übertragung vorgenommen wurde, wenn eine vorgebbare Bewertung

— der elektronischen Belege, deren Nichtübertragung Betrug ermöglicht, insbesondere entsprechend Anzahl oder einem diesem Belegen entsprechenden Buchgeldbetrag und/oder

— der elektronischen Belege, deren Übertragung einen wirtschaftlichen Nutzen für den Betreiber des Endgerätes erbringen, insbesondere entsprechend Anzahl oder einem diesem Belegen entsprechenden Buchgeldbetrag

nicht mehr erfüllt ist.

12. Verfahren nach Patentanspruch 11 dadurch gekennzeichnet, daß die Sperrung sich nur auf solche Anwendungen mit mobilen Datenträgern bezieht, die einen Betrug ermöglichen.

13. Verfahren nach Patentansprüchen 11 und 12 dadurch gekennzeichnet, daß die Sperrung aufgehoben wird, falls die vorgebbare Bewertung durch höhere gespeicherte Buchgeldbeträge aus nicht gesperrten Anwendungen wieder erfüllt ist.

14. Verfahren gemäß Oberbegriff von Anspruch 1 dadurch gekennzeichnet, daß ein Datenträger für weitere Anwendungen gesperrt wird, bis entsprechende Übertragungen an das Abrechnungs-/Kontoführungssystem vorgenommen wurde, wenn eine vorgebbare Bewertung bisher vorgenommener Anwendungen, welche zu Betrug genutzt werden können, nicht mehr erfüllt ist, insbesondere Bewertungen entsprechend Anzahl oder einem diesem Anwendungen entsprechenden Buchgeldbetrag.

15. Verfahren nach Patentanspruch 14 dadurch gekennzeichnet, daß die Sperrung sich nur auf Anwendungen bezieht, welche zu Betrug genutzt werden können.

16. Verfahren nach Patentansprüchen 15 und 3 dadurch gekennzeichnet, daß die Bewertung aktualisiert wird, indem erkannte Übertragungen an das Abrechnungs-/Kontoführungssystem berücksichtigt werden, und eine Sperrung des Datenträgers dadurch aufgehoben wird.

17. Verfahren nach vorstehenden Ansprüchen dadurch gekennzeichnet, daß gespeicherte, elektronische Belege aus Endgeräten, welche nicht dauerhaft an das Abrechnungs-/Kontoführungssystem angeschlossen sind, bei der Anwendung transportabler Datenträger in diese zur Weiterleitung an das Abrechnungs-/Kontoführungssystem gespeichert werden, wobei der Beleg nicht mit dem Datenträger oder seinem Inhaber in Zusammenhang stehen muß.

– Leerseite –